

## CLAIMS

What is claimed is:

1 1. A method comprising:  
2 producing a pseudonym including a public pseudonym key within a  
3 platform;  
4 placing the public pseudonym key into a certificate template;  
5 performing a hash operation on the certificate template to produce a  
6 certificate hash value;  
7 performing a transformation on the certificate hash value for transmission  
8 from the platform;  
9 receiving a signed result being a digital signature for the transformed  
10 certificate hash value; and  
11 performing an inverse transformation on the signed result to recover a  
12 digital signature of the certificate hash value.

1 2. The method of claim 1, wherein the producing of the pseudonym  
2 includes generating the public pseudonym key and a private pseudonym key  
3 corresponding to the public pseudonym key.

1 3. The method of claim 1, wherein the placing of the public  
2 pseudonym key into the certificate template includes writing the public  
3 pseudonym key into a field of the certificate template.

1 4. The method of claim 1, wherein the performing of the  
2 transformation comprises:  
3 performing a logical operation on the certificate hash value using a  
4 pseudo-random number to produce a value differing from the certificate hash  
5 value.

1 5. The method of claim 4, wherein the pseudo-random number is a  
2 predetermined value raised to an inverse power designated by a pseudo-random  
3 value.

1 6. The method of claim 5, wherein the pseudo-random value is stored  
2 in secure memory.

1 7. The method of claim 4, wherein the performing of the inverse  
2 transformation comprises performing a logical operation on the signed result  
3 using an inverse of the pseudo-random number.

1 8. The method of claim 1, wherein prior to receiving the digital  
2 signature, the method comprises:  
3 digitally signing a certification request, including the transformed  
4 certificate hash value, with a private key of a first platform to produce a signed  
5 certification request.

1 9. The method of claim 8, wherein prior to receiving the digital  
2 signature, the method further comprises:  
3 obtaining a device certificate being a digital certificate chain that includes  
4 a public key of a first platform, to accompany the signed certificate request

1 10. The method of claim 9, wherein prior to receiving the digital  
2 signature, the method further comprises:  
3 transferring the signed certificate request and the device certificate to a  
4 second platform.

1 11. The method of claim 11 further comprising:  
2 storing the digital signature of the certificate hash value for use in  
3 subsequent communications to a remotely located platform.

1 12. A device comprising:  
2 a processing unit; and  
3 a persistent memory including a first key pair and at least one pseudonym  
4 for use in communications with a remotely located device and in identifying that a  
5 platform containing the device is secure.

1 13. The device of claim 12, wherein the at least one pseudonym  
2 includes a second key pair.

1 14. The device of claim 13, wherein the second key pair is erased after  
2 a communication session with the remotely located device has concluded.

1 15. The device of claim 12 further comprising:  
2 a number generator to assist in producing the at least one pseudonym.

1 16. A platform comprising:  
2 a transceiver; and  
3 a device in communication with the transceiver, the device including a  
4 persistent memory to contain a permanent key pair, at least one pseudonym  
5 generated internally within the device and a digital signature of a hash value of a  
6 digital certificate chain that includes a public pseudonym key of the pseudonym.

1 17. The platform of claim 16, wherein the device further includes:  
2 a processing unit to (i) write the public pseudonym key into a certificate  
3 template, (ii) perform a hash operation on the certificate template to produce a  
4 certificate hash value, (iii) to perform a transformation operation on the certificate  
5 hash value.

1 18. The platform of claim 17, wherein the processing unit of the device  
2 further produces a digital signature of at least the transformed certificate hash  
3 value using a private key of the permanent key pair.

1 19. The platform of claim 16, wherein the processing unit of the device  
2 further appending a device certificate with the digital signature of at least the  
3 transformed certificate hash value.

1 20. The platform of claim 19, wherein the device certificate is the  
2 digital certificate chain.